

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans VMware

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-215>

---

### Gestion du document

Référence	CERTA-2012-AVI-215
Titre	Vulnérabilité dans VMware
Date de la première version	16 avril 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMMSA-2012-0007 du 12 avril 2012
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Contournement de la politique de sécurité.

## 2 Systèmes affectés

- Workstation 8.0.1 et antérieures ;
- Player 4.0.1 et antérieures ;
- ESXi 5.0 (sauf le correctif ESXi500-201203102-SG) ;
- ESXi 4.1 (sauf le correctif ESXi410-201201402-BG) ;
- ESXi 4.0 (sauf le correctif ESXi400-201203402-BG) ;
- ESXi 3.5 (sauf le correctif ESXi350-201203402-T-TG) ;
- ESX 4.1 (sauf le correctif ESX410-201201401-SG) ;
- ESX 4.0 (sauf le correctif ESX400-201203401-SG) ;
- ESX 3.5 (sauf le correctif ESX350-201203402-BG).

### **3 Résumé**

Une vulnérabilité a été corrigée dans les produits *VMware*. La vulnérabilité permet d'élever ses droits dans une machine *Windows* virtualisée. Cette exploitation peut être réalisée à cause des permissions appliquées au répertoire utilisé par *VMware Tools*.

### **4 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

### **5 Documentation**

- Bulletin de sécurité VMware VMSA-2012-0007 du 12 avril 2012 :  
<http://www.vmware.com/security/advisories/VMSA-2012-0007.html>
- Référence CVE CVE-2012-1518 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1518>

### **Gestion détaillée du document**

**16 avril 2012** version initiale.